테스트베드 구축을 통한 디지털계측제어계통 사이버보안 평가 방법에 관한 연구

차기종*, 신요순*, 서달미*, 손창호*, 김영미**, 정충희**
*㈜엔에스이
**한국원자력안전기술원
e-mail:kjcha@nsetec.com

A Study on Cyber Security Evaluation Method of the Digital Instrument and Control System using the Construction of a Test-bed

Ki-Jong Cha*, Yo-Soon Shin*, Chang-Ho Sohn*, Dal-Mi Seo*, Young-Mi Kim**, Choong-Heui Jeong**
*Next Solutions for Engineering and Technology Ltd.
**Korea Institute of Nuclear Safety

요 약

최근 디지털계측제어시스템은 사이버위협에 매우 취약하여 사이버공격에 의해 발전소 안전에 부정적인 영향을 받을 수 있는 실정이다. 따라서 디지털계측제어시스템에 대해 주기적인 사이버보안 위험 평가가 필요하다. 이에 따라 본 논문에서는 테스트베드 구축을 통해 특정 시점에서의 사이버 위협의 침해 가능성 분석, 또는 자체적으로 사이버보안성을 평가할 수 있는 방법에 대해 제안한다. 동 연구에서 제안하는 사이버보안 위험 평가는 자산분석, 테스트베드 구축, 취약점 분석, 위협평가, 위험도분석 및 평가 총 5단계로 구성되며 각 단계의 사이버보안 활동 수행을 통해 디지털계측제어계통의 사이버보안 수준이 향상될 것으로 사료된다.

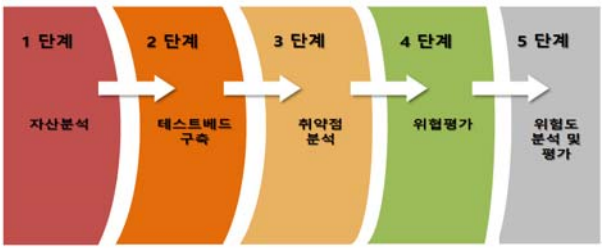
1. 서론

원자력발전소의 계측제어시스템은 90년대 중반까지 대부분 아날로그 방식으로 설계 및 운영되어 왔으나 아날로그 기반 시스템의 가동 연수 증가로 인한 성능 저하, 이에 따른 유지보수 비용의 증대, 대체품목의 단종 등은 원자력발전소의 계측제어 시스템을 정상적으로 운영하는데 심각한 현안사항으로 대두되어왔다. 이에 따라 최근 신규 건설되는 국내외 원전의 계측제어 시스템은 모두 디지털 기술을 바탕으로 설계 및 운영되고 있으며 아날로그 기반 시스템의 단점을 보완하고 안전하고 효율적으로 운전될 수 있도록 지원하고 있다. 그러나 이러한 순기능적 측면에 반하여 디지털계측제어시스템은 사이버위협에 매우 취약하여 사이버공격에 의해 발전소 안전에 부정적인 영향을 받을 수 있다. 더욱이 현재 디지털계측제어시스템 사이버보안에 대한 국내 연구체계는 부재한 상황으로 국내 디지털계측제어시스템 환경에 맞는 디지털계측제어시스템 사이버보안 위험 평가 방법을 마련하고 이를 활용할 수 있도록 하는 등의 적극적인 사전 연구 및 대응이 필요한 시점이라고 할 수 있다.

이러한 배경을 토대로, 본 논문에서는 디지털계측제어시스템에 대해 주기적인 사이버보안 위험 평가를 위해 테스트베드(Test-bed)를 구축하고 이에 대한 침투시험(Penetration Test)을 통해 특정 시점에서의 사이버 위협의 침해 가능성 분석 또는 자체적으로 사이버보안성을 평가할 수 있는 방법에 대해 연구하고 기술한다.

2. 사이버보안 위험 평가 방법

본 연구에서 제시하는 디지털계측제어시스템의 사이버보안 위험 평가 방법은 그림 1과 같이 크게 5단계로 구분된다.



(그림 1) 사이버보안 위험 평가 단계

1단계의 자산분석에서는 사이버보안의 적용 대상 계통의 특성과 구성을 파악함을 목적으로 한다. 2단계의 테스트베드 구축에서는 현장에서 사용되는 장치들의 사양과 기능 그리고 통신 규약 및 계층 구조를 반영하여 구성된다. 3단계의 취약점 분석에서는 수집된 정보를 기반으로 세부점검항목을 도출하고 대상 시스템이 가진 취약점을

분석, 평가한다. 4단계의 위협평가에서는 대상 시스템에 대해 존재하는 위협을 식별하고 분석하는 단계이며 실질적인 모의침투시험을 수행한다. 5단계의 위험도평가 및 분석에서는 식별된 보호대상 자산에 대한 취약점, 위협평가 결과를 기반으로 위험도를 산정하여 보호 대상 자산을 보호하기 위한 사이버 보안 요건을 도출한다.

2.1 자산분석

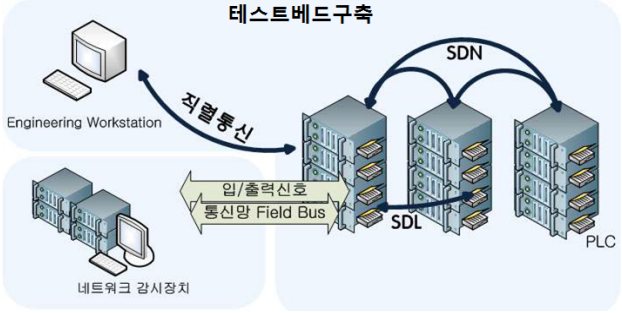
자산분석은 자산의 가치 및 중요도를 산출하며, 자산에 대한 침입 또는 손상에 대한 위험분석 결과의 정확도를 결정하는 중요한 과정이다. 또한, 자산에 필요한 사이버보안 요건을 식별하고 이에 적합한 사이버보안 활동을 도출하기 위한 사전분석 활동이다. 그림 2는 자산분석 절차별 수행해야할 내용과 각 절차에서의 입력과 출력을 나타낸다[1].

(그림 2) 자산분석 절차별 입력 및 출력

2.2 테스트베드 구축

보안성 평가를 위해 테스트베드는 여러 가지 형태의 통신장애와 침입 및 교란 공격 등에 대한 모의가 가능하도록 설계되며, 보안성 평가 수행을 위하여 다음에 나열한 해킹(hacking) 방법들의 모의가 가능하여야 한다[2].

- 위장하기(spoofing)
- 재생공격(reply attack)
- 서비스거부(DoS, Denial of Service)
- 세션 하이재킹(session hijacking)
- 스니핑(sniffing)



(그림 3) 디지털계측제어계통 테스트베드의 구조

2.3 취약점분석

정부 및 기업체에서 일반적으로 사용하는 정보시스템의 사이버보안 통제를 위해서는 미국 국립표준기술연구소에서 발간한 NIST SP800-53을 준용하고 있다. NIST SP800-53은 연방정부 행정기관을 지원하는 정보시스템에 대한 보안평가를 선택 및 지정할 수 있는 지침 제공을 목적으로 하는 권고안이다[3]. 반면에, 일반적인 정보시스템의 보안과는 달리 산업제어시스템에 대한 보안 사항은 NIST SP800-82에서 다루어지고 있다[4].

원자력발전소의 디지털계측제어시스템도 산업에서 전반적으로 쓰이고 있는 산업제어시스템의 일종으로 볼 수 있다. 일반적인 산업제어시스템이 가지고 있는 사이버보안 취약점은 더 엄격한 보안을 요구하는 원자력발전소의 디지털계측제어계통에도 적용이 가능하므로 본 연구에서는 NIST SP800-82에서 다루는 취약점을 대상으로 대상 시스템이 가진 취약점을 분석, 평가하여 대상 자산의 보안수준을 평가하고 위험평가를 위한 기반 정보를 제공하는 활동을 수행하였다. NIST SP800-82에서는 제어시스템에서 발견될 수 있는 잠재적인 취약점 목록을 대응전략 수립이 용이하도록 정책 및 절차, 플랫폼, 네트워크로 분류하여 제시한다.

2.3.1 정책 및 절차의 취약점 점검항목

디지털계측제어시스템과 관련된 사이버 보안 문서, 구현 지침 등 정책 및 절차의 존재 유무와 내용상 적절성 확인을 통해 취약점을 점검한다.

정책 및 절차와 관련된 취약점은 다음과 같다.

- ICS에 대한 부적절한 보안정책
- 공식적인 보안교육 및 인지프로그램의 부재
- 부적절한 보안구조 및 설계
- 설정된 ICS 보안정책에 근거한 보안절차의 부재 또는 비구체화
- ICS 장비 구현을 위한 지침서의 부재 및 결함
- 보안 실행을 위한 행정절차의 부족
- ICS에 대한 보안감사의 부재 또는 부족
- ICS의 재난극복계획 및 구체화된 연속운전계획의 부재
- ICS에 특화된 구성변화관리 프로그램의 부족

2.3.2 플랫폼의 취약점 점검항목

디지털계측제어시스템에서 사용되는 하드웨어 및 소프트웨어에 대한 오류, 잘못된 설정 및 부적절한 유지관리 여부에 대한 확인을 통해 취약점을 점검한다.

플랫폼 구성과 관련된 취약점은 다음과 같다.

- 보안취약점이 발견된 이후에도 운영체제 및 벤더 소프트웨어의 패치가 개발되지 않음
- 운영체제 및 응용프로그램의 패치가 유지되지 않음
- 철저한 시험 없이 운영체제 및 응용프로그램의 패치가 구현됨

- 기본 구성을 사용함
- 필수적인 구성이 저장되지 않거나 백업되지 않음
- 휴대용 장치의 보호되지 않은 데이터
- 적절한 패스워드 정책의 부족
- 패스워드를 사용하지 않음
- 패스워드 노출
- 패스워드 추측
- 부적절한 접근제어 방법 적용

2.3.3 네트워크의 취약점 점검항목

디지털계측제어시스템을 구성하는 네트워크에 대한 오류, 잘못된 설정 및 부적절한 유지관리 여부 또는 다른 네트워크와의 연결 여부에 대한 확인을 통해 취약점을 점검한다.

네트워크 구성과 관련된 취약점은 다음과 같다.

- 네트워크의 보안구조가 빈약한 경우
- 데이터 흐름제어를 적용하지 않은 경우
- 빈약하게 구성된 보안장비의 사용
- 네트워크 장비의 구성 파일을 저장 및 백업하지 않은 경우
- 암호화하지 않은 패스워드 전송
- 네트워크 장비에 계속 존재하는 패스워드
- 부적절한 접근제어를 적용한 경우

네트워크 하드웨어와 관련된 취약점은 다음과 같다.

- 네트워크 장비에 대한 부적절한 물리적 방호
- 안전하지 않은 물리적 포트의 사용
- 환경 통제의 부재
- 필수적이지 않은 인원들이 네트워크 연결 및 장비에 접근하는 경우
- 필수적인 네트워크의 중복성 부족

네트워크 경계와 관련된 취약점은 다음과 같다.

- 보안 경계가 정의되지 않은 경우
- 방화벽이 설치되지 않았거나 부적절하게 구성된 경우
- 제어네트워크에서 비 제어 트래픽을 사용한 경우
- 제어네트워크가 아닌 영역에서 제어네트워크 서비스를 사용한 경우

네트워크 감시 및 로깅과 관련된 취약점은 다음과 같다.

- 방화벽 및 라우터의 부적절한 로그
- ICS 네트워크상에서 보안감시를 하지 않는 경우

통신과 관련된 취약점은 다음과 같다.

- 필수적인 감시 및 제어 경로가 정의되지 않은 경우
- 표준화 및 문서화된 통신프로토콜 적용 시 평문을 사용하는 경우
- 사용자, 데이터 및 장비의 인증에 열악한 방법을 사용하는 경우
- 통신 시 무결성 확인이 부족한 경우

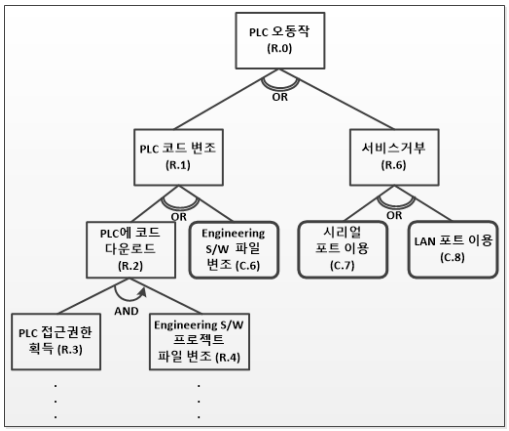
무선 연결과 관련된 취약점은 다음과 같다.

- 클라이언트와 AP 간의 부적절한 인증 방법을 사용하는 경우
- 클라이언트와 AP 간의 부적절한 데이터 방어 방법을 사용하는 경우

2.4 위협평가

위협평가에서는 대상 시스템에 대해 존재하는 위협을 식별하고 분석하여 위협의 실현 가능성과 위협이 실현되었을 때 보호대상 시스템이 받을 예상 영향도를 평가하는 단계이다. 위협평가의 단계는 위협소스 식별, 공격트리 구성, 공격 트리 분석, 모의침투수행으로 총 4단계로 구성된다.

1단계에서는 취약점 및 위협 정보를 기반으로 시스템에 위협이 될 수 있는 위협 소스 식별 활동을 수행한다. 2단계에서는 수집 또는 분석된 자산 및 연결, 의존성 정보와 자산평가 결과를 바탕으로 대상 시스템에 대한 가상의 공격 경로를 표현하는 공격트리를 구성한다. 공격 트리의 개념은 공격자의 최종 행위 결과로부터 출발하여 결과의 발생을 가능케 한 원인들을 탐색하고, 각각의 확인된 원인으로부터 단계적으로 더 근본적인 원인으로 거슬러 올라가는 과정을 반복함으로써 결국에는 잠재적인 시스템취약점에 대해 충분히 세분화된 윤곽을 파악하게 되어 그에 상응한 대응책을 마련할 수 있다는 것이다[5].



(그림 4) 침투시험을 위한 공격트리 구조

3단계 공격트리분석에서는 자산 및 취약점에 대한 분석결과를 기반으로 구성된 공격트리에서 표현되는 공격경로의 실현 가능성 및 영향도를 분석하는 활동을 수행한다. 4단계 모의침투에서는 보다 실질적인 가능성 및 영향도를 평가하기 위하여 공격트리를 이용한 모의침투시험을 수행한다.

2.5 위험도평가 및 분석

위험도평가 및 분석에서는 모의침투시험을 통해 분석된 공격 시나리오를 기반으로 각 노드와 노드들의 조합으로 구성된 시나리오에 대한 공격 가능성과 영향도를 평가하여 위험도를 산정한다. 위험도를 산정하기 위해 공격 가능성 수준(attack Possibility Level, PL)과 영향도 수준(Consequence Level, CL)값을 기준으로 사용하며 2가지의 특성값은 공격트리를 구성하는 각 노드들에 부여되며, 그 값들을 기반으로 최상위 노드인 최종 공격 목표의 위험도를 산정한다[6].

공격 가능성 수준 값은 다음과 같다. 기 정의된 위협소스가 공격 트리내의 각 노드를 공격할 수 있는 가능성 수준을 표현하며 PL 값은 총 5단계로 분류된다. 각 단계의 판단 기준은 표 1과 같다.

<표 1> 공격 가능성 수준(attack Possibility Level, PL)

구분	표현	설명
P5	Very High	모의침투를 통한 침투성공
P4	High	침투성공 가능성 높음 (취약점 진단을 통해 공격시나리오에 대한 위협의 존재가 확인된 취약점 발견)
P3	Moderate	침투성공 가능성 존재. (공격시나리오에 대한 알려진 취약점이 존재하고 해당 취약점에 대한 위협이 존재)
P2	Low	침투성공 가능성 낮음
P1	Very Low	침투 불가능

영향도 수준 값은 공격 트리 내의 각 노드가 침해당했을 경우, 그 영향이 다른 노드들에 미칠 수 있는지 여부를 표현한다. 영향도 수준은 자산 분석 단계의 결과인 영향성 평가(Confidentiality, Integrity, Availability) 결과를 기반으로 산정되며 그 기준은 표 2와 같다. 원전의 디지털계측제어시스템은 일반적인 산업제어 시스템과 유사하게 기밀성보다는 상대적으로 무결성과 가용성이 더 중요시된다. 이러한 산업 제어 시스템의 특성이 영향도 수준 분류 기준에 반영되었다.

<표 2> 영향도 수준(Consequence Level, CL)

구분	표현	설명
C5	Very High	시스템의 무결성과 가용성에 영향을 주어 발전소 운영에 심각한 영향을 줄 수 있음
C4	High	시스템의 무결성과 가용성에 심각한 영향을 줄 수 있음
C3	Mode-rate	시스템의 무결성과 가용성에 보통의 영향을 줄 수 있음
C2	Low	시스템의 무결성과 가용성에 적은 영향을 줄 수 있음
C1	Very Low	시스템의 무결성과 가용성에 거의 영향을 주지 않음

마지막으로 위험도 수준 값을 할당하기 위해 우선, 각 시나리오에 속한 노드들에 PL 값과 CL 값을 부여하고, 그 값을 이용하여 표 3의 기준표에 의해 SRL(Security Risk Level)값이 할당된다.

<표 3> 위험도 수준(Security Risk Level, SRL)

PL/CL	C5	C4	C3	C2	C1
PL5	SRL5	SRL5	SRL5	SRL5	SRL5
PL4	SRL5	SRL5	SRL4	SRL4	SRL3
PL3	SRL5	SRL5	SRL3	SRL3	SRL3
PL2	SRL4	SRL3	SRL2	SRL2	SRL2
PL1	SRL2	SRL2	SRL1	SRL1	SRL1

3. 결론

디지털 계측제어시스템은 순기능적 측면에 반하여 사이버위협에 매우 취약하여 사이버공격에 의해 발전소 안전에 부정적인 영향을 받을 수 있다. 이에 따라 본 논문에서는 국내 디지털계측제어시스템 환경에 맞는 디지털계측제어시스템 사이버보안 위험 평가 방법을 마련하고 이를 활용할 수 있도록 하는 테스트베드 구축을 통한 디지털계측제어계통의 사이버보안 평가 방법을 제안하였다.

디지털계측제어시스템의 사이버보안 위험 평가 방법은 크게 5단계이며 자산분석, 테스트베드 구축, 취약점 분석, 위협평가, 위험도 분석 및 평가로 구성된다. 제안한 방법은 디지털계측제어시스템에 잠재되어 있는 사이버 취약성을 제거하여 가동 중 및 신규 원전의 사이버보안 수준을 향상 시키며 안전 운전을 가능토록 하는데 적용될 것으로 기대된다.

차후 연구 과제로는 현재 제어시스템 사이버보안을 위한 테스트베드 구축에 대한 국내 연구체계는 부재한 상황이므로 향후 효율적인 제어 시스템 테스트베드 구축을 위한 연구가 수행되어야 할 것으로 사료된다.

참고문헌

[1] 구인수, 김관웅, “원자력발전소의 디지털계측제어시스템의 사이버보안을 위한 디지털 자산분석 방법,” 한국전자통신학회논문지, 6권, 6호, pp839-847, 2011.

[2] 이종주, 김석주, 강동주, “SCADA 시스템의 보안성 평가를 위한 테스트베드 구성,” Journal of KIEE, vol.24, No4, April 2010.

[3] NIST SP 800-53, “Recommended Security Controls for Federal Information System,” National Institute of Standards and Technology, 2009.

[4] NIST SP 800-82, “Guide to Industrial Control System(ICS) Security,” National Institute of Standards and Technology, 2008.

[5] 김경아, 이대성, 김귀남, “공격 트리를 이용한 산업 제어 시스템 보안 위험 분석,” 한국사이버테러정보전학회, 11권, 6호, 2011.

[6] NIST SP 800-30, “Risk Management Guide for Information Technology Systems,” National Institute of Standards and Technology, 2012.